Overview of MGCP and Related Protocols

This chapter provides overview information on Media Gateway Control Protocol (MGCP) and related protocols.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for MGCP and Related Protocols

- Configure IP routing.
- Configure voice ports.
- Configure VoIP.
- Configure the call agent. (For information on setting up call agents, see the documentation that accompanies the call agents used in your network configuration.)

Information About MGCP and Related Protocols

MGCP is an extension of the earlier version of the protocol Simple Gateway Control Protocol (SGCP) and supports SGCP functionality in addition to several enhancements. Systems using SGCP can easily migrate to MGCP, and MGCP commands are available to enable SGCP capabilities.

An MGCP gateway handles translation between audio signals and the packet network. Gateways interact with a call agent (CA)--also called a media gateway controller (MGC)--that performs signal and call processing on gateway calls. In the MGCP configurations that Cisco IOS supports, a gateway can be a Cisco router, access server, or cable modem, and the CA is a server from a third-party vendor.

Configuration commands for MGCP define the path between the call agent and the gateway, the type of gateway, and the type of calls handled by the gateway.

MGCP uses endpoints and connections to construct a call. Endpoints are sources of or destinations for data, and can be physical or logical locations in a device. Connections can be point-to-point or multipoint.

Similar to SGCP, MGCP uses User Datagram Protocol (UDP) for establishing audio connections over IP networks. However, MGCP also uses hairpinning to return a call to the PSTN when the packet network is not available.

Package Types

A call connection involves a series of events and signals--such as off-hook status, a ringing signal, or a signal to play an announcement--that are specific to the type of endpoint involved in the call.

MGCP groups these events and signals into packages. A trunk package, for example, is a group of events and signals relevant to a trunking gateway; an announcement package is a group of events and signals relevant to an announcement server. MGCP supports the following seven package types:

- Trunk
- Line
- Dual-tone multifrequency (DTMF)
- Generic media
- Real-Time Transport Protocol (RTP)
- Announcement server
- Script

The trunk package and line package are supported by default on certain types of gateways. Although configuring a gateway with additional endpoint package information is optional, you may want to specify packages for your endpoints to add to or override the defaults.

Protocol Benefits

MGCP provides the following benefits:

- Alternative dial tone for VoIP environments--Deregulation in the telecommunications industry gives competitive local-exchange carriers (CLECs) opportunities to provide toll bypass from the incumbent local-exchange carriers (ILECs) by means of VoIP. MGCP enables a VoIP system to control call setup and teardown and Custom Local Area Subscriber Services (CLASS) features for less sophisticated gateways.
- Simplified configuration for static VoIP network dial peers--When you use MGCP as the call agent in a VoIP environment, you need not configure static VoIP network dial peers. The MGCP call agent provides functions similar to VoIP-network dial peers.

Note Plain old telephone service (POTS) dial peer configuration is still required.

- Migration paths--Systems using earlier versions of the protocol can migrate easily to MGCP.
- Varied network needs supported for the following:
  - Interexchange carriers (IXCs) who have no legacy time-division multiplexing (TDM) equipment in their networks and want to deploy a fully featured network that offers both long-distance services to corporate customers and connectivity to local exchange carriers or other IXCs with traditional TDM equipment.
  - IXCs who have TDM equipment in their networks and want to relieve network congestion using data technologies to carry voice traffic or to cap the growth of TDM ports. In these situations, the packet network provides basic switched trunking without services or features.
  - Competitive competitive local-exchange carriers (CLECs) who want to provide residential and enhanced services.
  - Dial-access customers who want enhanced Signaling System 7 (SS7) access capabilities and increased performance, reliability, scalability, and economy.

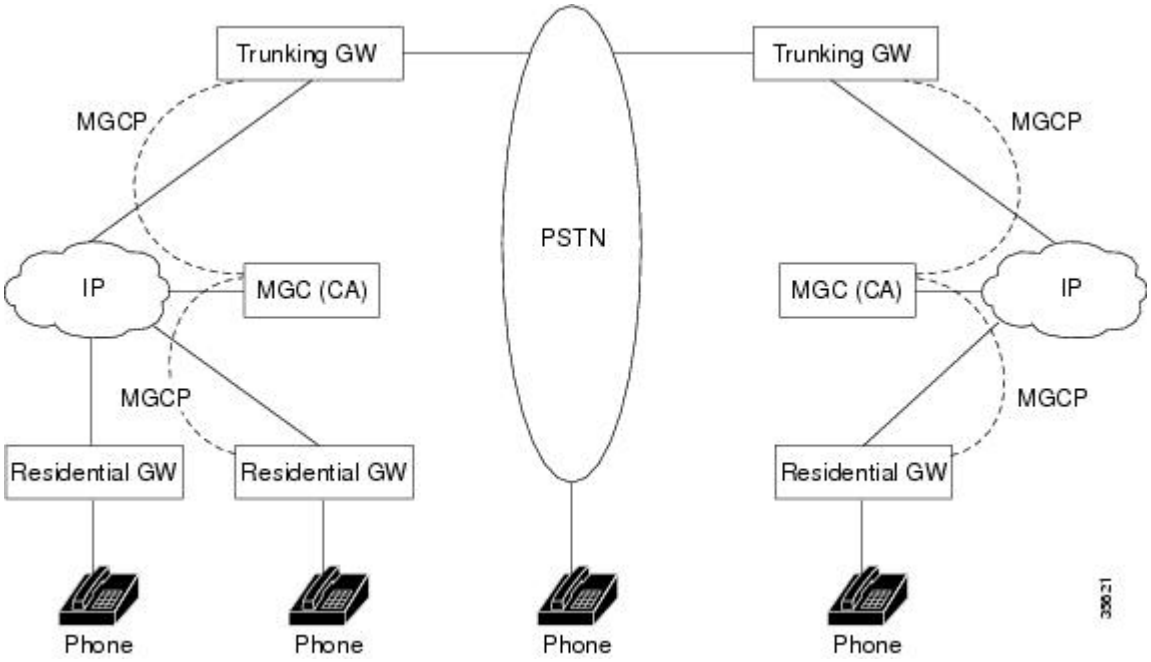
Supported Gateways

MGCP supports both residential and trunking gateways.

Residential Gateway

A residential gateway (RGW) provides an interface between analog (RJ-11) calls from a telephone and the VoIP network. Examples of RGWs include cable modems and Cisco 2600 series routers. The figure below shows an RGW configuration.

Figure 1: Residential and Trunking Gateways



RGW functionality supports analog POTS calls for both SGCP and MGCP on the Cisco 2600 series routers and Cisco uBR924 cable access router as shown in the table below.

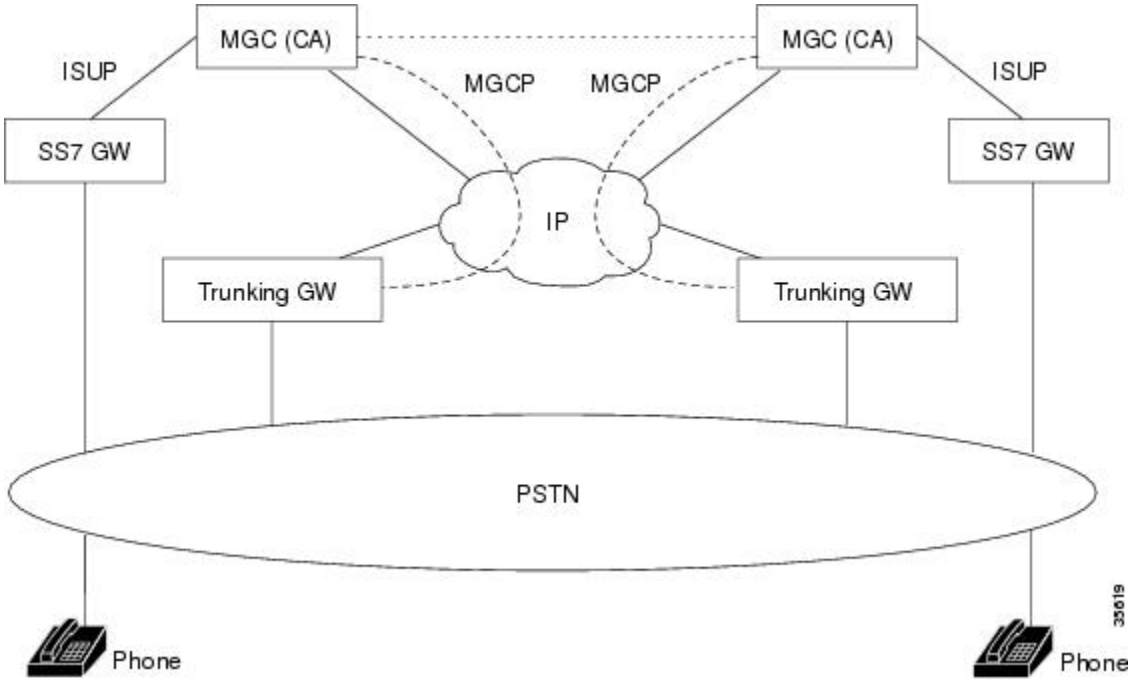
Table 1: RGW Functionality

Functionality	Platform	
Cisco 2600 Series	Cisco uBR924	
Call waiting	Yes	Yes
Default call-agent address specifiable for each foreign exchange station (FXS) port	--	Yes
Distinctive ringing	--	Yes
Fax and modem calls	Yes	Yes
On-hook caller identification (ID)	--	Yes
Ring splash	--	Yes
Stutter dial tone	Yes	Yes

Trunking Gateway

A trunking gateway (TGW) provides an interface between PSTN trunks and a VoIP network. A trunk can be a DS0, T1, or E1 line. Examples of TGWs include access servers and routers. The figure below shows a TGW configuration.

Figure 2: Trunking Gateways



TGW functionality supports SGCP and MGCP as shown in the table below.

Table 2: TGW Functionality

Functionality	Platform	
Cisco AS5300	Cisco 3660	
911 outgoing calls on T1 lines	Yes[1]	
Fax and modem calls	Yes	Yes
PRI/ISDN signaling (calls are backhauled to the call agent)	Yes	
SS7	Yes	Yes
T1 and E1 interfaces	Yes	Yes

[1] Server must have SGCP 1.1+ protocol for Feature Group D Operator Services (FGD-OS)

Toll Fraud Prevention

When a Cisco router platform is installed with a voice-capable Cisco IOS software image, appropriate features must be enabled on the platform to prevent potential toll fraud exploitation by unauthorized users. Deploy these features on all Cisco router Unified Communications applications that process voice calls, such as Cisco Unified Communications Manager Express (CME), Cisco Survivable Remote Site Telephony (SRST), Cisco Unified Border Element (UBE), Cisco IOS-based router and standalone analog and digital PBX and

public-switched telephone network (PSTN) gateways, and Cisco contact-center VoiceXML gateways. These features include, but are not limited to, the following:

- Disable secondary dial tone on voice ports--By default, secondary dial tone is presented on voice ports on Cisco router gateways. Use private line automatic ringdown (PLAR) for foreign exchange office (FXO) ports and direct-inward-dial (DID) for T1/E1 ports to prevent secondary dial tone from being presented to inbound callers.
- Cisco router access control lists (ACLs)--Define ACLs to allow only explicitly valid sources of calls to the router or gateway, and therefore to prevent unauthorized Session Initiation Protocol (SIP) or H.323 calls from unknown parties to be processed and connected by the router or gateway.
- Close unused SIP and H.323 ports--If either the SIP or H.323 protocol is not used in your deployment, close the associated protocol ports. If a Cisco voice gateway has dial peers configured to route calls outbound to the PSTN using either time division multiplex (TDM) trunks or IP, close the unused H.323 or SIP ports so that calls from unauthorized endpoints cannot connect calls. If the protocols are used and the ports must remain open, use ACLs to limit access to legitimate sources.
- Change SIP port 5060--If SIP is actively used, consider changing the port to something other than well-known port 5060.
- SIP registration--If SIP registration is available on SIP trunks, turn on this feature because it provides an extra level of authentication and validation that only legitimate sources can connect calls. If it is not available, ensure that the appropriate ACLs are in place.
- SIP Digest Authentication--If the SIP Digest Authentication feature is available for either registrations or invites, turn this feature on because it provides an extra level of authentication and validation that only legitimate sources can connect calls.
- Explicit incoming and outgoing dial peers--Use explicit dial peers to control the types and parameters of calls allowed by the router, especially in IP-to-IP connections used on CME, SRST, and Cisco UBE. Incoming dial peers offer additional control on the sources of calls, and outgoing dial peers on the destinations. Incoming dial peers are always used for calls. If a dial peer is not explicitly defined, the implicit dial peer 0 is used to allow all calls.
- Explicit destination patterns--Use dial peers with more granularity than .T for destination patterns to block disallowed off-net call destinations. Use class of restriction (COR) on dial peers with specific destination patterns to allow even more granular control of calls to different destinations on the PSTN.
- Translation rules--Use translation rules to manipulate dialed digits before calls connect to the PSTN to provide better control over who may dial PSTN destinations. Legitimate users dial an access code and an augmented number for PSTN for certain PSTN (for example, international) locations.
- Tcl and VoiceXML scripts--Attach a Tcl/VoiceXML script to dial peers to do database lookups or additional off-router authorization checks to allow or deny call flows based on origination or destination numbers. Tcl/VoiceXML scripts can also be used to add a prefix to inbound DID calls. If the prefix plus DID matches internal extensions, then the call is completed. Otherwise, a prompt can be played to the caller that an invalid number has been dialed.
- Host name validation--Use the "permit hostname" feature to validate initial SIP Invites that contain a fully qualified domain name (FQDN) host name in the Request Uniform Resource Identifier (Request URI) against a configured list of legitimate source hostnames.
- Dynamic Domain Name Service (DNS)--If you are using DNS as the "session target" on dial peers, the actual IP address destination of call connections can vary from one call to the next. Use voice source

groups and ACLs to restrict the valid address ranges expected in DNS responses (which are used subsequently for call setup destinations).

For more configuration guidance, see the " Cisco IOS Unified Communications Toll Fraud Prevention " paper.

Additional References

The following sections provide references related to MGCP.

Related Documents

Related Topic	Document Title
Cisco IOS configuration examples	Cisco Systems Technologies website at http://cisco.com/en/US/tech/index.html . Select a technology category and subsequent hierarchy of subcategories. Click **Technical Documentation > Configuration Examples**.
Cisco IOS debug command reference	*Cisco IOS Debug Command Reference*
Cisco IOS troubleshooting information	*Cisco IOS Voice Troubleshooting and Monitoring Guide*
Cisco IOS voice command reference	*Cisco IOS Voice Command Reference*

MIBs

MIBs	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport